# *Volenti non fit injuria*: Ransomware and its Victims

Amir Atapour-Abarghouei, Stephen Bonner and Andrew Stephen McGough
School of Computing, Newcastle University, Newcastle, UK
{amir.atapour-abarghouei, stephen.bonner3, stephen.mcgough}@newcastle.ac.uk

***Abstract*—With the recent growth in the number of malicious activities on the internet, cybersecurity research has seen a boost in the past few years. However, as certain variants of malware can provide highly lucrative opportunities for bad actors, significant resources are dedicated to innovations and improvements by vast criminal organisations. Among these forms of malware, ransomware has experienced a significant recent rise as it offers the perpetrators great financial incentive. Ransomware variants operate by removing system access from the user by either locking the system or encrypting some or all of the data, and subsequently demanding payment or *ransom* in exchange for returning system access or providing a decryption key to the victim. Due to the ubiquity of sensitive data in many aspects of modern life, many victims of such attacks, be they an individual home user or operators of a business, are forced to pay the ransom to regain access to their data, which in many cases does not happen as renormalisation of system operations is never guaranteed. As the problem of ransomware does not seem to be subsiding, it is very important to investigate the underlying forces driving and facilitating such attacks in order to create preventative measures. As such, in this paper, we discuss and provide further insight into variants of ransomware and their victims in order to understand how and why they have been targeted and what can be done to prevent or mitigate the effects of such attacks.**

***Index Terms*—Ransomware, Malware, Cybersecurity, Cryptography, Taxonomy.**

## I. Introduction

With the growing influence of automated data handling systems in various aspects of the daily life of an average citizen, such as banking, education, health care and many other public and private services, systems security is becoming ever more important. Various malicious online activities by large criminal syndicates or independent individual bad actors now threaten any operation reliant on computer systems.

Of the numerous strains of malware regularly appearing online, ransomware is now of particular interest to the cybersecurity community [1] as it is capable of targeting any user indiscriminately and can inflict irreversible harm on its victims. A ransomware often exploits low-level operating system mechanisms or security-based operations, such as cryptography, to isolate users from their assets (be these data services or systems), partially or on the whole. The user can only regain access if and when a sometimes-hefty "ransom" is paid, and in many instances, the access to the data is never returned to the user even if the ransom is paid in full [2]. Consequently, due to the significant financial gain ransomware can offer the perpetrators [3], considerable resources are often put behind

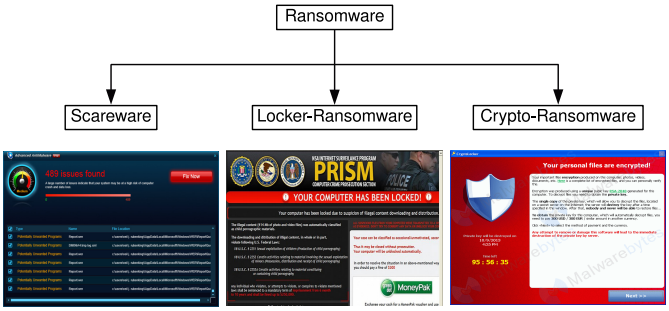


Fig. 1: Types of ransomware grouped by attack intensity.

the creation of new and innovative variants, allowing them to bypass state-of-the-art anti-virus and anti-malware software [4].

Initially, ransomware attacks seem to have been in the form of *spray-and-prey*, with little targeting towards any particular individual. However, more recently, attackers have been moving towards more targeted attacks [5] – the so-called "big game hunting", in which cybercriminals target high-value organisations, putting significant value into identifying more targeted routes of entry.

As a result of this perceived high value for cybercriminals, the cybersecurity community has had to stay vigilant to maintain the ability to detect and avert constantly-emerging ransomware attacks. Malware activities have conventionally been identified either at the network level [6], [7], system level [8] or both [9]. For instance, Andronio [10] proposes an approach that identifies device-locking or encryption activities at the system level by finding code paths using static taint analysis along with symbolic execution. In another work, anomalous file system activities are used to detect ransomware [11]. Similarly, Scaife *et al.* [12] attempts to identify abnormal system behaviour by carefully measuring changes in file type, similarity measurements and entropy.

With the significant recent advances in machine learning [13]–[18], learning-based approaches have also found their way into the expansive literature on ransomware detection and classification. For example, the approach proposed by Sgandurra *et al.* [19] detects and classifies ransomware variants by dynamically analysing the behaviour of applications during the early stages of their installation. Ransomware classification has also been attempted through combining a static detection

*Volenti non fit injuria*: No wrong is done to one who consents.

978-1-7281-0858-2/19/$31.00 

phase based on the frequency of opcodes prior to installation and a dynamic method which investigates the use of CPU, memory and network as well as call statistics during runtime [20]. Vinayakumar *et al*. [21] investigates the efficacy of neural networks used to detect and classify ransomware activities, with a focus on tuning the hyperparameters and the architecture of a simple multilayer perceptron. In another work, Atapour *et al*. [22] propose a vision-based system that classifies ransomware variants based on an image of the splash screen casually captured using a smartphone camera.

Despite the advances in ransomware detection techniques, the constantly-evolving landscape of ransomware and the substantial level of diversity among its variants give further importance to acquiring deeper insight into the nature of ransomware attacks. In this vein, we take a closer look at ransomware categories and particularly the types of victims that are often targeted and regularly fall for ransomware attacks. In Section II, we briefly review the types of ransomware commonly found in the wild, Section III focuses on the victims of ransomware attacks and finally, a number of preventative and response strategies are discussed in Section IV.

## II. Variants of Ransomware

Before attempting to understand the victims of ransomware attacks, it is important to understand the varieties of ransomware and the reasons behind this variation. While the existing literature contains numerous studies that provide meaningful taxonomies of ransomware [23]–[26], we primarily focus on aspects of ransomware variants that can directly contribute to a deeper understanding of their victims.

Ransomware variants can be classified based on their mode of propagation (*e.g*. through pre-packaged exploitation kits [27], affiliate packages built on top of existing malware infrastructures [28], spam campaigns [28]), payment methods (*e.g*. direct digital currency payments [29], pre-paid vouchers, calls and texts to premium rate numbers, online purchases) and many other characteristics. However, of the numerous factors that can aid in the classification of ransomware with respect to the victims: attack intensity [23], [24] and the user platform towards which the attack is designed [26] are arguably the most important. Considering these factors, we provide a very generic classification of ransomware variants in the following.

### A. Attack Intensity

In terms of the intensity of the attacks (the level of threat a ransomware can pose to an infected system), there are, in general, three types of ransomware: scareware, locker-ransomware and crypto-ransomware (Figure 1).

Predominantly, the objective of a scareware is simply to scare the victim into paying a fee without causing any actual harm to the computer system [30] and can thus be easily dealt with. This is usually accomplished by displaying a fake splash screen on the victim's computer [22] and asking for a ransom despite the files and the entire system still being accessible to the user. In most cases, a scareware might threaten the victim by alleging that they have found illegal content or viral infections on the system [31], [32] and exploit the victim's fear to extort money.

Conversely, locker-ransomware and crypto-ransomware [7] can be truly detrimental to system, sometimes causing irreparable damage. Locker-ransomware often takes control of the locking capabilities of the operating system and denies the victim access to one or more of the system services or applications [30]. The system is subsequently left with limited capabilities, which might only allow the victim to follow the instructions needed to pay the ransom. However, this form of ransomware is, in many cases, incapable of successfully extorting the ransom, especially from skilled PC users, as the operating system and the files are left intact and unharmed and it is relatively easy to bypass the locking mechanism.

Crypto-ransomware, on the other hand, employs cryptography to encrypt the user's files [33], essentially removing all access to the files, leaving the victim with two options: either pay the ransom or forever lose access to all the encrypted files (which in many cases will happen even if the ransom is paid). In essence, the ransom is demanded in exchange for the decryption key, which is often the only way for the victim to regain access to the data and/or the system.

When it comes to the profile of the victims targeted by these types of ransomware, technical knowledge often plays a critical role. While highly-skilled victims are unlikely to pay the ransom, except for cases where a crypto-ransomware has successfully encrypted files which have not been archived or backed up, unskilled users can fall victim to locker-ransomware or even scareware. However, depending on the platform, these variants of ransomware can have different effects and can cause varying levels of harm. As such, in the following section, we focus on the platforms different variants of ransomware might target.

### B. Target Platform

Another factor that plays a role in understanding the ransomware victims is the platform they use. While PCs and mobile devices have long been the target of ransomware attacks, new variants of ransomware now commonly attack IoT devices and cloud-based systems as well [34]. There has even been a demonstration that other consumer devices such as digital cameras can also be successfully targeted [35]. Encrypting images directly on the camera could have significant negative impact, especially if the photographer is working as a professional.

However, due to the wide-spread use of personal computers for decades, it is expected that they make up the majority of ransomware targets, and while MS Windows systems are most commonly attacked, others such as Mac OS and Linux machines are not entirely immune either [36], [37]. PCs are often targeted by all three types of ransomware (scareware, locker-ransomware and crypto-ransomware), with the number of attacks being on the rise and new variants constantly being introduced [38], [39].

Due to the ease of use and the low skill levels needed to operate, mobile devices are now ubiquitously used by a

wide spectrum of individuals, making them ideal targets for ransomware attacks [40], [41]. Mobile ransomware attacks have reportedly more than quadrupled since 2015 [42], with locker-ransomware variants carrying out most of the successful attacks. This is mainly due to the fact that important personal files are often kept outside the mobile device, rendering local encryption attacks against the device useless, and the mobile operating systems do not offer the manoeuvrability needed to bypass a locking attack, making them significantly more effective [26] than locking attacks against a PC.

Recently, there have been numerous reports of attacks on IoT devices [43], despite such appliances generally not holding any valuable data. Not unlike mobile attacks, different variants of locker-ransomware can inflict significant harm to the users of IoT devices by disabling access, causing power outages and even disrupting critical services [38]. To understand why and how certain victims are targeted more often than others, in the next section, we focus on the victims, themselves.

## III. Ransomware Victims

Since significant financial gain continuously drives the creation and spread of ransomware [3], one of the most effective methods of combating this type of malware is cutting off the supply of funds obtained through the ransom paid by the victims. Hence, a deeper understanding of the typical victims of ransomware attacks can be very helpful in coming up with solutions that prevent or mitigate the current fast-growing ransomware problem. From a top-down perspective, ransomware victims can broadly be classified into two wide groups: individuals and business entities. Due to the important differences between these two groups, the behaviour of the ransomware targeting these victims is often very different.

### A. Individual Home Users

Consumer ransomware often targets individual home users, which in terms of numbers make up the majority of ransomware victims [26]. These individualistic attacks are often opportunistic and perpetrated via indiscriminate attack vectors. For instance, the victim might receive a spam e-mail, in which they are encouraged to click on a malicious link or they might visit a compromised website infecting the system with ransomware. In rarer occasions, however, infection can occur without user engagement through drive-by downloads [44] or by means of malvertising and ad-injections [45].

Considering the limited resources often available to non-technical individual victims compared to large corporations and government-affiliated organisations, the ransom demanded from the victims is often significantly smaller ($300 to $700) [38]. When a consumer ransomware attacks a targeted individual, all the files and resources are normally locked or encrypted as fast as computationally possible and the ransom note is quickly displayed in the form of a splash screen [22]. Despite the more affordable fees demanded by the perpetrators, due to the large number of infections a single attack can spread across the world, this type of ransomware attack remains profitable and incentivises further investment of resources and development for the perpetrators [46].

Non-technical individuals are also widely targeted by scareware (Section II-A), the variants of which essentially issue fake warnings and threaten the victim's files and/or personal privacy without them ever actually being in any serious danger. For instance, the famous FakeAV [47] epitomises a typical scareware by adopting the appearance of a legitimate anti-virus that warns the user of the supposedly malicious software it has discovered on the victim's computer after a fake scan. Subsequent to the this, payment is demanded, sometimes very aggressively, to remove the fake malware [30].

With the growth of the *ransomware-as-a-service* model [48], even unskilled amateur hackers are now capable of launching ransomware attacks using pre-fabricated automated tools, which sometimes come with a consumer support service to talk the victims through negotiation attempts and payments [49]. This has a led to an increase in the number of mass indiscriminate attacks against individuals, necessitating a deeper analysis and understanding of the situation. While certain factors such as age, level of education and financial resources do contribute to the likelihood of an individual falling victim to a ransomware attack and subsequently paying the ransom, the level of computer-literacy is the primary determining factor.

While simple solutions such as regular software and operating system updates [30], [50], e-mail security (on both client and server side [50], [51]), anti-malware tools [52], access and authorisation control [53] and simply backing up the data [54], [55] can significantly reduce the number of successful ransomware attacks on individuals, the user needs to be aware of and skilled enough to implement such measures, which signifies the value of computer-literacy for the public.

### B. Business Entities

Despite having access to large IT infrastructures and security professionals, business organisations also regularly fall victim to ransomware attacks. Such ransomware attacks are often a consequence of the more targeted (big game hunting) attacks where the perpetrator may put significant effort into preparing a credible social attack against an identified member of staff. After gaining access through an entry point into the system, the attack vectors often employed by such ransomware variants are mostly gradual and covert [38]. The ransomware usually focuses on avoiding and evading the countermeasures deployed by the organisation's security experts and slowly takes control of specifically targeted data, such as transactional documents, backups and archives [26]. As expected, large organisations often receive significantly higher ransom demands compared to individuals, easily reaching numbers as high as $10,000 or higher [26].

As far as business entities and organisations are concerned, the security systems, the type of data and possibly the services they deal with are the primary factors in their victimisation. In the following, we focus on the various sectors that are often targeted by ransomware attacks.

*1) Education:* In recent years, educational institutions, such as schools and universities, have become one of the primary targets of ransomware attacks. In fact, according to a recent report [56], the educational sector faces the largest number of attacks per capita with more than 10% of all schools and universities having been targeted. Many such organisations have budgetary constraints, limited access to cybersecurity professionals and smaller teams of often over-worked IT personnel, yet due to their high rate of network file sharing and centralised systems [57] can be prime targets for any malware.

Additionally, an average school, university or any other educational or research institute stores valuable and highly-sensitive data on students, who might be under the legal age, staff, intellectual property, financial documents and sometimes even medical records that must not be compromised in any way. One such ransomware attack was experienced by University College London, where shared drives and student management systems were compromised [58] in 2017.

*2) Health Industry:* Healthcare facilities and hospitals are also commonly targeted for ransomware attacks, mainly due to the highly critical data and services that they depend on. Not having immediate access to a patient's data can have life-or-death consequences. A major example of this would be the Hollywood Presbyterian Medical Center, where a ransom of $3.7 million was demanded after highly-sensitive medical data and hospital services were disrupted. The hospital was forced to pay the ransom since daily administrative operations were reduced to pen and paper, and more importantly, the life of the patients was hanging in the balance. This case, however, is particularly notable as the ransom was negotaited down to $17,000 and access to the data and services was returned to the hospital [53] allowing normal operations to resume.

*3) Government Agencies:* The number of attacks on government agencies tripled from 2015 to 2016 [56] and has been steadily growing ever since. In 2018, the city of Atlanta, Georgia suffered a significant ransomware attack. The ransomware had found its entry point into the system by means of a brute-force attack to crack weaker passwords [59]. Although most services (safety, water and airport operations) were not compromised, online payment systems and court information access were severely restricted, potentially affecting up to 6 million people [59] and costing the city over $2.7 million in recovery efforts.

As government agencies are generally perceived to have significantly larger funds available to them and many of their services (*e.g.* police, water, transportation) are highly critical and time-sensitive, perpetrators always look for opportunities to get through the security systems of such organisations in any way possible.

*4) Utilities, Retail and Finance:* With the growing reliance many organisations in the utilities, retail and finance sector place on computationally-powerful low-latency systems, combined with the significantly heavy costs they can suffer as a result of any down-time, they have become one of the recurring targets of ransomware attacks [56]. In many such companies, and even small to mid-size businesses of similar nature, the human resources departments are now regularly preyed on as they often have access to many other sections and departments within any given company and this connectivity is very enticing to the perpetrators [60].

*5) Emerging Targets:* In general, any organisation that holds sensitive data or offers critical services is always at risk of a ransomware attack. A law firm, for instance, is always in danger. While the loss of data can be catastrophic to a law firm, the possibility of publicising confidential client data can put an end to the business entirely, which would make a law firm willing to pay any amount [57]. Industrial control systems have also largely avoided being targets of ransomware attacks [61], but this is not because of their level of security as there are glaring security vulnerabilities that do not seem to be improving [30]. Any widespread attack on such systems can lead to a compromise in critical infrastructure, which can have devastating international consequences.

## IV. Prevention and Response

Since the significant re-emergence of ransomware within the past few years, many new tools and workarounds have been suggested to mitigate or recover from a ransomware attack. However, due to the increasing viability of the business model, perpetrators invest significant resources to stay ahead of the cybersecurity community. According to a recent report [62], the number of ransomware attacks that have been successfully detected and prevented saw a 30% increase from 2015 to 2016. However, the overall number of attacks has also notably risen. Consequently, detecting every new variant of ransomware might be impossible using a single powerful anti-malware tool, but there are various techniques that individuals or companies can employ to protect their systems from a ransomware infection. Here, we discuss certain measures that can help with the prevention of or response to a ransomware attack. In Section IV-A, we discuss some of the most prominent security techniques that can prevent ransomware attacks and in Section IV-B, we focus on what should be done in response to an infection.

### A. Prevention Techniques

Attempting to remove a ransomware or re-gaining access to a corrupted system or encrypted data can be very expensive and sometimes impossible, even if the ransom is paid. The best solution, in this case, is prevention. While securing the system and network activity is extremely important for both individual users and business organisations, an overwhelming majority of successful malware attacks are due to human error [63], so securing the end user is of utmost importance. In the following, we briefly outline the most important prevention approaches on the system and the user side.

*1) Network/System Security:* While certain system and network security measures are more expensive and require expert support, the majority of the recommendations listed below apply to both individual home users and business entities:

- A robust backup and archiving system removes the threat the majority of ransomware attacks can pose.

- Anti-malware and other similar tools are indispensable to a secure system. Modern tools [52] even take advantage of machine learning approaches to remove their dependence on knowledge of existing threat signatures.
- In a secure system, all hardware, operating systems, software, cloud locations and content management systems must be patched and up-to-date at all times.
- Via effective system administration, application whitelisting and software restriction policies [64], dubious programs can be kept off the system, specially for large companies, where controlling and monitoring all the employees with system access might not be possible.
- Using a proxy-server and any of the numerous ad-blocking packages, common ransomware entry points can be restricted.
- Through network segmentation, virtual machines, and limited authorisation and privileges, potentially harmful network access to sensitive data can be averted.
- It is important for any organisation, to introduce access policies and closely monitor any third parties as they can easily introduce vulnerabilities into the system.
- Any company with sensitive data requires a response plan that outlines how the system can be protected if an attack is detected in its early stages.

*2) End User Security:* While human error is a significant cause of ransomware attacks [63], it is not always avoidable. Nor can we assume that a well-constructed attack would not thwart even the most security-savvy. Education and training, both for individuals and businesses with many employees, can be very effective in preventing, or at least reducing the likelihood of, a ransomware attack.

- End users need to be aware of social engineering as it is a common attack vector for many malicious actors [65].
- All end users must be trained on phishing and how it must be countered.
- Companies should have strict policies about their employees' use of the internet as personal emails and social media websites [66] are regular points of entry for many ransomware variants.
- It is very important for end users to have strong passwords as perpetrators can easily gain access to the main system via various password cracking approaches [67].

### B. Response to an Attack

More often than not, when data has been encrypted using a crypto-ransomware, not many solutions are left available. However, it is very important, especially for non-skilled individuals, to ensure the infection has indeed been caused by a crypto-ransomware as locker-ransomware and scareware can often be easily removed from most computer systems without causing serious harm to the system.

Identification is often key when seeking to distinguish which type of Ransomware has infected the system. In such situations, knowledge is highly-important especially as many attackers obfuscate their ransomware to reduce the chance of easy detection. The "No More Ransom" project [68] provides a mechanism to identify the ransomware from either the text within the ransom note or a small number of the encrypted files. While Atapour *et al*. offers a more layperson approach allowing users to take a picture of the ransomware splash screen and use this for identification [22].

In cases where the algorithm or the key used by the perpetrators are not strong, a decryption solution might be available. While certain companies such as Kaspersky and Windows Defender offer proprietary decryption tools, the *No More Ransom* project [68] is specifically dedicated to helping all victims, whether individual home users or businesses, to recover their encrypted files without having to pay the ransom.

Finally, one of the most important actions every business entity or individual home user must take after a ransomware infection is to report the incident and share as much data about the incident as possible with the authorities and experts. Many individuals and companies often remain quiet about such attacks out of fear of bad publicity. However, reporting such events can go a long way in putting a stop to similar future attacks.

## V. Conclusion

The level of threat that ransomware poses is extremely serious and can disrupt the fabric of our modern data-dependent society. With the recent rise in cybercrime, it is now more important than ever to combat the perpetrators of ransomware attacks and cut off the large supply of funds regularly invested in the development and improvement of new variants of ransomware. In this vein, this paper has primarily focused on facilitating a better understanding of ransomware variants and the victims often targeted by them. We also provide a brief classification of ransomware variants and the attack vectors they are commonly associated with. This is accomplished by examining the severity of the threat a variant of ransomware can pose and the platform it is designed to attack. The paper also discusses the targets predominantly victimised by ransomware perpetrators to enable further insight into the underlying forces that drive this malicious business model. While individual home users make up the majority of the victims, depending on the type of data they hold or the services they may provide, businesses can make for more lucrative targets and are often at a greater risk. Furthermore, we have briefly considered helpful prevention strategies for individuals and businesses that fall victim to these attacks and the potential post-infection recovery techniques that might aid in mitigating the devastating effects the loss of sensitive data can have on any victim as paying the ransom is rarely advisable and is not guaranteed to lead to a full recovery of the data.

## Acknowledgement

This work was in part supported by the EPSRC EMPHASIS (EP/P01187X/1) and CRITiCaL (EP/M020576/1) projects.

## References

[1] H. Zhang, X. Xiao, F. Mercaldo, S. Ni, F. Martinelli, and A. K. Sangaiah, "Classification of ransomware families with machine learning based on N-gram of opcodes," *Future Generation Computer Systems*, vol. 90, pp. 211–221, 2019. 1

[2] C. Moore, "Detecting ransomware with honeypot techniques," in *Cybersecurity and Cyberforensics Conference*. IEEE, 2016, pp. 77–81. 1

[3] A. Laszka, S. Farhang, and J. Grossklags, "On the economics of ransomware," in *Int. Conf. Decision and Game Theory for Security*. Springer, 2017, pp. 397–417. 1, 3

[4] S. Kok, A. Abdullah, N. Jhanjhi, and M. Supramaniam, "Ransomware, threat and detection techniques: A review," *Int. J. Computer Science and Network Security*, vol. 19, no. 2, p. 136, 2019. 1

[5] "High-impact ransomware attacks threaten U.S. businesses and organisations," https://www.ic3.gov/media/2019/191002.aspx. 1

[6] G. Gu, R. Perdisci, J. Zhang, and W. Lee, "Botminer: Clustering analysis of network traffic for protocol and structure independent Botnet detection," *USENIX Security Symposium*, 2008. 1

[7] K. Cabaj, M. Gregorczyk, and W. Mazurczyk, "Software-defined networking-based crypto ransomware detection using HTTP traffic characteristics," *Computers & Electrical Engineering*, vol. 66, pp. 353–368, 2018. 1, 2

[8] U. Bayer, P. M. Comparetti, C. Hlauschek, C. Kruegel, and E. Kirda, "Scalable, behavior-based malware clustering," in *Network and Distributed System Security Symposium*, vol. 9, 2009, pp. 8–11. 1

[9] G. Jacob, R. Hund, C. Kruegel, and T. Holz, "JACKSTRAWS: Picking command and control connections from Bot traffic," in *USENIX Security Symposium*, 2011. 1

[10] N. Andronio, "Heldroid: Fast and efficient linguistic-based ransomware detection," Ph.D. dissertation, 2015. 1

[11] A. Kharraz, W. Robertson, D. Balzarotti, L. Bilge, and E. Kirda, "Cutting the gordian knot: A look under the hood of ransomware attacks," in *Int. Conf. Detection of Intrusions and Malware, and Vulnerability Assessment*. Springer, 2015, pp. 3–24. 1

[12] N. Scaife, H. Carter, P. Traynor, and K. R. Butler, "Cryptolock (and drop it): Stopping ransomware attacks on user data," in *Int. Conf. Distributed Computing Systems*. IEEE, 2016, pp. 303–312. 1

[13] K. Simonyan and A. Zisserman, "Very deep convolutional networks for large-scale image recognition," *arXiv preprint arXiv:1409.1556*, 2014. 1

[14] A. Atapour-Abarghouei and T. P. Breckon, "Real-time monocular depth estimation using synthetic data with domain adaptation via image style transfer," in *IEEE Conf. Computer Vision and Pattern Recognition*, 2018, pp. 2800–2810. 1

[15] S. Ren, K. He, R. Girshick, and J. Sun, "Faster R-CNN: Towards real-time object detection with region proposal networks," in *Advances in Neural Information Processing Systems*, 2015, pp. 91–99. 1

[16] T. Mikolov, I. Sutskever, K. Chen, G. S. Corrado, and J. Dean, "Distributed representations of words and phrases and their compositionality," in *Advances in Neural Information Processing Systems*, 2013, pp. 3111–3119. 1

[17] A. Grover and J. Leskovec, "node2vec: Scalable feature learning for networks," in *Int. Conf. Knowledge Discovery and Data Mining*. ACM, 2016, pp. 855–864. 1

[18] S. Bonner, J. Brennan, I. Kureshi, G. Theodoropoulos, A. S. McGough, and B. Obara, "Temporal graph offset reconstruction: Towards temporally robust graph representation learning," in *IEEE Int. Conf. Big Data*, 2018, pp. 3737–3746. 1

[19] D. Sgandurra, L. Muñoz-González, R. Mohsen, and E. C. Lupu, "Automated dynamic analysis of ransomware: Benefits, limitations and use for detection," *arXiv preprint arXiv:1609.03020*, 2016. 1

[20] A. Ferrante, M. Malek, F. Martinelli, F. Mercaldo, and J. Milosevic, "Extinguishing ransomware - A hybrid approach to Android ransomware detection," in *Int. Symp. Foundations and Practice of Security*. Springer, 2017, pp. 242–258. 2

[21] R. Vinayakumar, K. Soman, K. S. Velan, and S. Ganorkar, "Evaluating shallow and deep networks for ransomware detection and classification," in *Int. Conf. Advances in Computing, Communications and Informatics*. IEEE, 2017, pp. 259–265. 2

[22] A. Atapour-Abarghouei, S. Bonner, and A. S. McGough, "A king's ransom for encryption: Ransomware classification using augmented one-shot learning and bayesian approximation," in *IEEE Int. Conf. Big Data*, 2019, pp. 1–6. 2, 3, 5

[23] X. Luo and Q. Liao, "Awareness education as the key to ransomware prevention," *Information Systems Security*, vol. 16, no. 4, pp. 195–202, 2007. 2

[24] ——, "Ransomware: A new cyber hijacking threat to enterprises," in *Handbook of Research on Information Security and Assurance*. IGI global, 2009, pp. 1–6. 2

[25] M. M. Ahmadian, H. R. Shahriari, and S. M. Ghaffarian, "Connection-monitor & connection-breaker: A novel approach for prevention and detection of high survivable ransomwares," in *Int. Iranian Society of Cryptology Conf. Information Security and Cryptology*. IEEE, 2015, pp. 79–84. 2

[26] B. A. S. Al-rimy, M. A. Maarof, and S. Z. M. Shaid, "Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions," *Computers & Security*, vol. 74, pp. 144–166, 2018. 2, 3

[27] M. Hopkins and A. Dehghantanha, "Exploit Kits: The production line of the cybercrime economy?" in *Int. Conf. Information Security and Cyber Forensics*. IEEE, 2015, pp. 23–27. 2

[28] J. Wyke, "The ZeroAccess Botnet–Mining and fraud for massive financial gain," *Sophos Technical Paper*, 2012. 2

[29] S. Higgins, "CoinDesk on Citrix survey, BTC stocks in UK businesses," https://www.coindesk.com/survey-uk-bitcoin-ransomware. 2

[30] K. Savage, P. Coogan, and H. Lau, "The evolution of ransomware," *Security Response: Symantec Corporation*, 2015. 2, 3, 4

[31] J.-L. Richet, "Extortion on the internet: the rise of crypto-ransomware," *Harvard*, 2016. 2

[32] P. Pathak and Y. M. Nanded, "A dangerous trend of cybercrime: Ransomware growing challenge," *Int. J. Advanced Research in Computer Engineering & Technology*, vol. 5, no. 2, pp. 371–373, 2016. 2

[33] N. Ganesh, F. Di Troia, V. A. Corrado, T. H. Austin, and M. Stamp, "Static analysis of malicious Java applets," in *Int. Workshop on Security And Privacy Analytics*. ACM, 2016, pp. 58–63. 2

[34] Symantec, "Internet security threat report," 2019. 2

[35] "Say cheese, ransomware-ing a DSLR camera," https://research.checkpoint.com/say-cheese-ransomware-ing-a-dslr-camera/. 2

[36] L. Arsene and A. Gheorghe, "Ransomware: A victim's perspective," *BitDefender*, 2016. 2

[37] R. Benchea, V. Cristina, M. Alexandru, and L. Arsene, "Petya ransomware goes low level," in *BitDefender*. BitDefender, 2016. 2

[38] J.-P. P., D. OBrien, and S. Wallace, "Ransomware and businesses," *An ISTR Special Report: Symantec Corporation*, 2016. 2, 3

[39] McAfee, "Threats predictions," *McAfee LLC.*, 2017. 2

[40] T. Yang, Y. Yang, K. Qian, D. C.-T. Lo, Y. Qian, and L. Tao, "Automated detection and analysis for Android ransomware," in *Int. Conf. High Performance Computing and Communications, Int. Symp. Cyberspace Safety and Security, and Int. Conf. Embedded Software and Systems*. IEEE, 2015, pp. 1338–1343. 3

[41] F. Afifi, N. B. Anuar, S. Shamshirband, and K.-K. R. Choo, "DyHAP: Dynamic hybrid ANFIS-PSO approach for predicting mobile malware," *PloS one*, vol. 11, no. 9, p. e0162627, 2016. 3

[42] K. Lab, "KSN report: Ransomware," 2016. 3

[43] A. Karkouch, H. Mousannif, H. Al Moatassime, and T. Noel, "Data quality in internet of things: A state-of-the-art ssurvey," *Journal of Network and Computer Applications*, vol. 73, pp. 57–81, 2016. 3

[44] M. Cova, C. Kruegel, and G. Vigna, "Detection and analysis of drive-by-download attacks and malicious JavaScript code," in *International Conference World Wide Web*. ACM, 2010, pp. 281–290. 3

[45] X. Xing, W. Meng, B. Lee, U. Weinsberg, A. Sheth, R. Perdisci, and W. Lee, "Understanding malvertising through ad-injecting browser extensions," in *Int. Conf. World Wide Web*. International World Wide Web Conferences Steering Committee, 2015, pp. 1286–1295. 3

[46] D. Bisson, "Half of American ransomware victims have paid the ransom," *TripWire*, 2017. 3

[47] B. Stone-Gross, R. Abman, R. A. Kemmerer, C. Kruegel, D. G. Steigerwald, and G. Vigna, "The underground economy of fake antivirus software," in *Economics of Information Security and Privacy III*. Springer, 2013, pp. 55–78. 3

[48] I. Nadir and T. Bakhshi, "Contemporary cybercrime: A taxonomy of ransomware threats & mitigation techniques," in *Int. Conf. Computing, Mathematics and Engineering Technologies*. IEEE, 2018, pp. 1–7. 3

[49] J. A. Sherer, M. L. McLellan, E. R. Fedeles, and N. L. Sterling, "Ransonware-practical and legal considerations for confronting the new economic engine of the dark web," *Rich. JL & Tech.*, vol. 23, p. 1, 2016. 3

[50] R. Leong, C. Beek, C. Cochin, N. Cowie, and C. Schmugar, "Understanding ransomware and strategies to defeat it," *White Paper (McAfee Labs)*, pp. 1–16, 2016. 3
[51] G. V. Cormack *et al.*, "Email spam filtering: A systematic review," *Foundations and Trends® in Information Retrieval*, vol. 1, no. 4, pp. 335–455, 2008. 3
[52] A. Continella, A. Guagnelli, G. Zingaro, G. De Pasquale, A. Barenghi, S. Zanero, and F. Maggi, "ShieldFS: A self-healing, ransomware-aware filesystem," in *Annual Conf. Computer Security Applications*. ACM, 2016, pp. 336–347. 3, 5
[53] T. A. Mattei, "Privacy, confidentiality, and security of health care information: Lessons from the recent Wannacry cyberattack," *World Neurosurgery*, vol. 104, pp. 972–974, 2017. 3, 4
[54] A. L. Young and M. Yung, "Cryptovirology: The birth, neglect, and explosion of ransomware," *Communications of the ACM*, vol. 60, no. 7, pp. 24–26, 2017. 3
[55] S. Mustaca, "Are your IT professionals prepared for the challenges to come?" *Computer Fraud & Security*, vol. 2014, no. 3, pp. 18–20, 2014. 3
[56] N. Simon, "The rising face of cybercrime: Ransomware," https://www.bitsight.com/blog/rising-face-of-cybercrime-ransomware. 4
[57] J. Martin, "Who is a target for ransomware attacks?" https://www.csoonline.com/article/3208111/who-is-a-target-for-ransomware-attacks.html. 4
[58] A. Hern, "University College London hit by ransomware attack," https://www.theguardian.com/technology/2017/jun/15/university-college-london-hit-by-ransomware-attack-hospitals-email-phishing. 4
[59] B. Freed, "Atlanta was not prepared to respond to a ransomware attack," https://statescoop.com/atlanta-was-not-prepared-to-respond-to-a-ransomware-attack. 4
[60] K. Zurkus, "Hackers prey on human resources using ransomware," https://www.csoonline.com/article/3112855/hackers-prey-on-human-resources-using-ransomware.html. 4
[61] D. Formby, S. Durbha, and R. Beyah, "Out of control: Ransomware for industrial control systems," in *RSA conference*, 2017. 4
[62] B. Nahorney, "Internet security threat report," 2017. 4
[63] Proofpoint, "The human factor 2019 report," https://www.proofpoint.com/us/resources/threat-reports/human-factor. 4, 5
[64] D. F. Sittig and H. Singh, "A socio-technical approach to preventing, mitigating, and recovering from ransomware attacks," *Applied Clinical Informatics*, vol. 7, no. 02, pp. 624–632, 2016. 5
[65] P. L. Gallegos-Segovia, J. F. Bravo-Torres, V. M. Larios-Rosillo, P. E. Vintimilla-Tapia, I. F. Yuquilima-Albarado, and J. D. Jara-Saltos, "Social engineering as an attack vector for ransomware," in *Chilean Conf. Electrical, Electronics Engineering, Information and Communication Technologies*. IEEE, 2017, pp. 1–6. 5
[66] R. Richardson and M. M. North, "Ransomware: Evolution, mitigation and prevention," *International Management Review*, vol. 13, no. 1, p. 10, 2017. 5
[67] S. Marechal, "Advances in password cracking," *Journal in Computer Virology*, vol. 4, no. 1, pp. 73–81, 2008. 5
[68] "No more ransomware project," https://www.nomoreransom.org/en/about-the-project.html. 5